White Paper: The Sarbanes-Oxley Act

Public Company Accounting Reform and Investment Protection Act

Sarbanes-Oxley Compliance: Pulling It All Together

***Abstract:** Few people are speaking about tangible approaches for information technology (IT) to meet the requirements of the Sarbanes-Oxley Act. This white paper provides some practical approaches and recommendations on how best to transform the new policies and procedures mandated by Sarbanes-Oxley into a working reality. It identifies the key technology areas enterprises must leverage to meet the stipulations of the Act, and offers "best practice" advice for a smoother implementation.*

FUJITSU
CONSULTING

Pulling It All Together: Collaboration Required

Executive Overview

The Sarbanes-Oxley (SOX) Act was passed in July 2002 to protect the investing public from officers of corporations and auditing firms who fraudulently misrepresent the financial stability of the corporation.

The Sarbanes-Oxley Act mandates accuracy in financial statements and disclosures to a level unprecedented in recent history. Certifying corporate officers must know, not just believe that their company's public financial statements are accurate and complete. The law also makes specific provisions for the retention of documents surrounding the audit process and public notifications due to material events.

There are a number of key provisions of the Act. One is good Control Point Management, which is more than just a "best practice"—the Act requires it through law. As of December 2003, organizations should be completing activities related to identifying and documenting their key processes and the Control Points related to these processes. Once Control Points are defined, the next step is to implement Control Point surveillance to instantly identify (and notify certifying offices) about unusual behavior ("material events"). To achieve these objectives, Fujitsu Consulting suggests the Fujitsu SOX Framework, which was constructed to meet the requirements placed upon IT by the Act. The Fujitsu SOX Framework encompasses your existing tools, monitoring practices, system automation routines and people to automate the surveillance of critical processes. Additionally, the framework bridges gaps in process monitoring, an essential element of achieving compliance.

The Fujitsu SOX Framework leverages IT in the areas of collaboration, reporting (real-time dashboards and reports), content collection and management, as well as your core business/financial applications. Further, you can be confident in the fact that the Fujitsu SOX Framework adheres to the principles of the Committee of Sponsoring Organizations (COSO).

Use of the Fujitsu SOX Framework also helps overcome the problem that no one person or group has the necessary knowledge to implement all the required aspects of SOX Control Point surveillance and material breach notification. Pulling together the correct team to accomplish your goals within a reasonable timeframe is important. The team must include individuals from diverse parts of the business to assure ready access to information for a quick, efficient, and effective SOX project. Obviously, the team must incorporate individuals with domain expertise in finance, business, legal, and technical disciplines.

Finally, the Fujitsu SOX Framework also helps ensure that "best practices" are utilized for threshold screening, filtering, and time delay for executive notifications. Incorporating filtering safeguards prevents rushed problem notifications to higher-level managers. This can be especially important for certifying officers, executive management, and internal/external auditors.

The Sarbanes-Oxley Act and the IT Organization: Background

The Sarbanes-Oxley Act leaves no room for certifying officers to claim "ignorance" to the possibility of creatively engineered financial figures. It also removes any ability to state "lack of knowledge" in overlooking unethical practices. Certifying corporate officers must know, not just believe, that their company's public financial statements are accurate and complete.

More specifically, SOX requires the documentation of internal processes, the establishment of internal controls and disclosure controls, plus the monitoring and documenting of these controls. The Act also establishes the requirement that evidence must be provided as to the effectiveness of these controls.

Business process owners and the IT organization must translate new policies and procedures—concerning monitoring, testing, documentation and reporting generated by SOX compliance activities—into a working reality. It falls upon the shoulders of process owners and IT to detect events surrounding Control Points, evaluate these events, ensure events are recorded for evidence, and perform notifications within 48 hours. It's easy to see that no one person or group has the necessary knowledge to implement all the required aspects of SOX Control Point surveillance and material breach notification. Pulling together the correct team to accomplish your goals within a reasonable timeframe is important.

SOX implementation is a team effort, and unlike Y2K, it is not going away at the stroke of midnight. The team that is assembled at this time will be the knowledge leaders for future modifications—which are inevitable.
At this point in the SOX compliance process (December 2003), your organization should be concluding project activities related to Section 302 of the Act, which establishes the need for detailed documentation of critical processes, and the identification of Control Points related to these processes. It has been our experience that analyzing processes, and capturing and documenting the "Who, What, Why, and Where" are some of the most difficult tasks. Assembling the right people, communicating the "Why" are we doing this, understanding "What" information is needed to monitor/capture, and "Where" the information resides are all critical success factors. Incorrectly performing these activities can lead to considerable expense to correct, and even result in jail time if done mischievously.

After establishing Control Points in accordance with Section 302, the follow-on steps are to establish monitoring (manual and/or automated) of the identified Control Points to comply with Sections 404 and 409. This is where the Fujitsu SOX Framework comes in.

Fujitsu Sarbanes-Oxley Framework Principles

The Fujitsu Sarbanes-Oxley Framework (Figure 1) was constructed to meet the requirements placed upon IT organizations by the Act. It was built to provide guidance for the many enterprises that are recognizing they do not have the surveillance infrastructure or workflow capabilities to adhere to Section 409 requirements. It also supports the requirement to alert executives of material events within 48 hours of their occurrence, as well as to store and manage evidence for years.

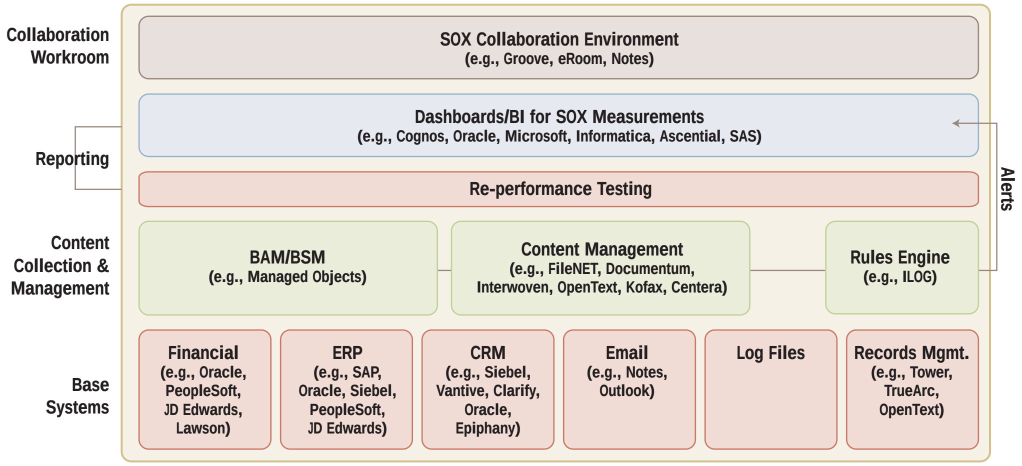

Collaboration Workroom
SOX Collaboration Environment
(e.g., Groove, eRoom, Notes)
Reporting
Dashboards/BI for SOX Measurements
(e.g., Cognos, Oracle, Microsoft, Informatica, Ascential, SAS)
Re-performance Testing
Alerts
Content Collection & Management
BAM/BSM
(e.g., Managed Objects)
Content Management
(e.g., FileNET, Documentum, Interwoven, OpenText, Kofax, Centera)
Rules Engine
(e.g., ILOG)
Base Systems
Financial
(e.g., Oracle, PeopleSoft, JD Edwards, Lawson)
ERP
(e.g., SAP, Oracle, Siebel, PeopleSoft, JD Edwards)
CRM
(e.g., Siebel, Vantive, Clarify, Oracle, Epiphany)
Email
(e.g., Notes, Outlook)
Log Files
Records Mgmt.
(e.g., Tower, TrueArc, OpenText)

Figure 1. Fujitsu Sarbanes-Oxley Framework

As illustrated, the Framework identifies the key technology areas enterprises must leverage to meet the stipulations of SOX. The Framework provides a clear picture and an integrated process for your organization's SOX compliance and reporting status.

The Base Systems depicted at the bottom of Figure 1 represent some of the key applications enterprises must monitor, and acquire data from, to assure Control Point validation and to detect fraudulent or suspicious activity. Surveillance also assures processes are operating and behaving as expected.

Next, Content Collection and Management applications work with, provide surveillance for, and manage the documented evidence related to your Control Points. Business Activity Monitoring/Business Systems Management software automates surveillance. An external rules engine could also be used in concert with Operational Data Stores (ODS) or Content Management software. Content Management software administers the process of maintaining documented evidence, document tracking and storage.

At the Reporting level of the framework, we have re-performance testing and use of dashboards. Re-performance refers to computations made to independently verify the integrity of transactions or balances. Re-performance testing also relates to testing the operating effectiveness of key controls. Re-performance testing can be accomplished through Business Applications Management/Business Systems Management (BAM/BSM) software or can be handled through a combination of manual and synthetic transactions. Either way, the approach and results must be captured and maintained for the auditors. Dissemination of information is most easily accomplished through dashboards and reports tailored for each stakeholder group. Reports and dashboards can be built and distributed with BAM/BSM, Content Management, and/or Business Intelligence software.

At the very top of the framework, in the Collaboration Workroom, collaboration software can be used by the project implementation team as well as virtual teams that may be assembled to investigate and resolve Control Point breaches.

What is a "Control Point"?

To understand how the Framework facilitates Control Point monitoring and management, it's important to level-set what we mean by "Control Points." SOX defines two types of controls: internal controls and disclosure controls.

An *internal control* is defined by the Committee of Sponsoring Organizations (COSO) as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the categories of:

1) Effectiveness and efficiency of operations
2) Reliability of financial reporting
3) Compliance with applicable laws and regulations

The first category, effectiveness and efficiency of operations, addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second category, reliability of financial reporting, relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third category, compliance with applicable laws and regulations, deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs.

A *disclosure control* is designed to ensure required information is acquired and disclosed. Exchange Act Rule 13a-15(d) further states that disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that the information required to be disclosed by a company in the reports that it files or submits under the Exchange Act are accumulated and communicated to the company's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure.

Controls are established to meet their objective (reliability of financial reporting) using recognized and repeatable criteria. Collectively, internal controls and disclosure controls are discussed in this white paper as Control Points.

Compliance with the Committee of Sponsoring Organizations Framework

The Fujitsu SOX Framework complies with the COSO framework and supports the five components shown on the face of the cube at the right in Figure 2.

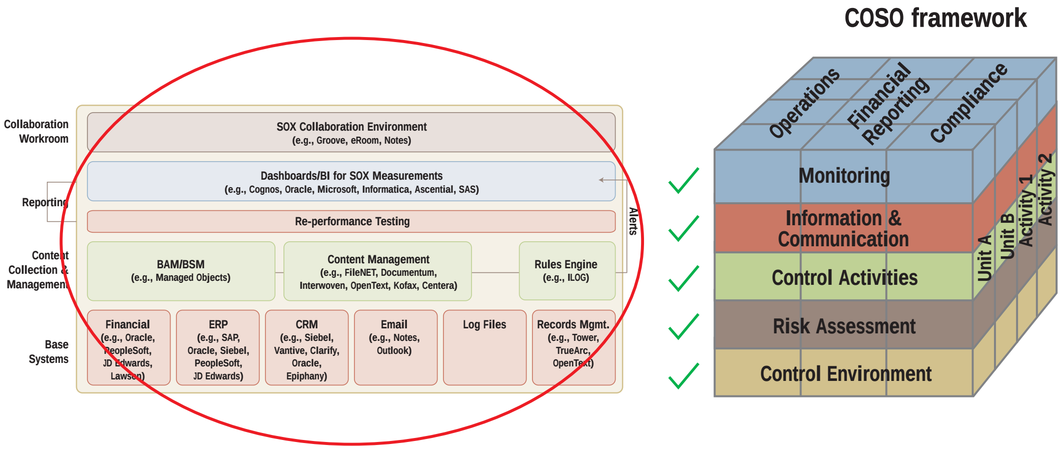

COSO framework
Collaboration Workroom
SOX Collaboration Environment
(e.g., Groove, eRoom, Notes)
Reporting
Dashboards/BI for SOX Measurements
(e.g., Cognos, Oracle, Microsoft, Informatica, Ascential, SAS)
Re-performance Testing
Alerts
Content Collection & Management
BAM/BSM
(e.g., Managed Objects)
Content Management
(e.g., FileNET, Documentum, Interwoven, OpenText, Kofax, Centera)
Rules Engine
(e.g., ILOG)
Base Systems
Financial
(e.g., Oracle, PeopleSoft, JD Edwards, Lawson)
ERP
(e.g., SAP, Oracle, Siebel, PeopleSoft, JD Edwards)
CRM
(e.g., Siebel, Vantive, Clarify, Oracle, Epiphany)
Email
(e.g., Notes, Outlook)
Log Files
Records Mgmt.
(e.g., Tower, TrueArc, OpenText)
Operations
Financial Reporting
Compliance
Monitoring
Information & Communication
Control Activities
Risk Assessment
Control Environment
Unit A
Unit B
Activity 1
Activity 2

Figure 2. Fujitsu-Sarbanes-Oxley Framework and the COSO framework

The five interrelated components are derived from the way management runs a business and are integrated with the management process. They are defined as follows:

1) Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The Fujitsu SOX Framework provides a control environment.

2) Risk Assessment: A pre-condition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. The detailed documentation built during Section 302 activities records critical processes and identifies Control Points to be monitored and tested as part of Section 404 dictates.

Associating metrics to Control Points and then establishing threshold values is a way to measure risk. Identifying appropriate threshold measurements are crucial for both real-time management and ongoing analysis of processes. Breaching a high or low threshold indicates something out of the ordinary is taking place. There may not actually be an issue, but it does deserve closer evaluation due to the implied risk that something is awry.

3) Control Activities: These constitute the policies and procedures to help ensure that management directives are carried out. They can pertain to both enterprise-wide and application-level controls for different organizational, functional, and systems activities.

Once the Control Points (identified and established in your Section 302 activities) are approved by management, you meet the initial requirements of this component. Defining the metrics to be monitored—as well as the baseline, average maximum, and average minimum values to be measured—establishes ongoing measurements to meet control activity requirements.

4) Information and Communication Dissemination: Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization.

Your implementation should leverage alerts and real-time dashboards, as well as reports to distribute information related to abnormal behavior and ongoing monitoring. It is important to:

- Deliver actionable information with dashboards and/or reports. Dashboards display a set of metrics that provide an "at-a-glance" information summary. The metrics may consist of information related to a single business process or provide an aggregated view of a number of business processes.
- Tailor information for the recipient or type of recipient.
- Use BAM/BSM, Content Management, Business Intelligence, as well as Collaboration software to build, store, and deliver information in dashboards or reports.

5) Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. The Fujitsu SOX Framework incorporates an automated means to monitor Control Points by BAM/BSM software, content management software, and/or rules engines.

Critical Success Factors to Consider

The Fujitsu SOX Framework ensures that critical success factors are not overlooked, such as:

- Risk management and enterprise-wide visibility
- Re-performance testing
- Use of dashboards and real-time reporting
- Use of collaboration software for verification, validation, and certification of Control Points

Each of these factors is discussed below.

Risk Management and Enterprise-Wide Visibility

Corporations typically manage risk in silos—by line of business, organizational entity, or location. The Framework provides an enterprise perspective for both the technical infrastructure and critical processes. This facilitates enterprise-wide tracking of loss events, Control Point surveillance, and impact reporting on operational risk losses to management.

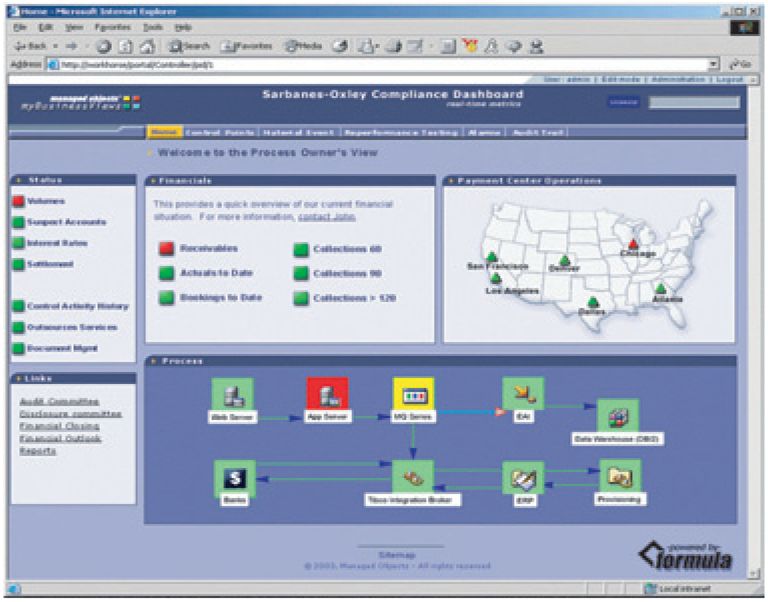
When every line-of-business measures and reports operational risk and control assessment differently, it can be difficult or impossible to gauge overall risk exposure and provide the disclosure required by Sarbanes-Oxley. The enterprise-wide perspective afforded by the Fujitsu SOX framework overcomes these traditional limitations, provides global visibility, and integrates critical processes across your organization to achieve SOX compliance for financial reporting.

Re-performance Testing

Re-performance refers to computations made to independently verify the integrity of transactions or balances. An example of this would be verifying a balance (such as number of parts, completed goods, or a bank balance.)

Re-performance testing also relates to testing the operating effectiveness of key controls. Documenting the results of tests and maintaining information as material evidence is important for your SOX efforts, as well as to meet audit requirements. Ongoing testing of the operating effectiveness of controls is necessary to meet audit committee and external auditor requests. Re-performance testing can be accomplished through synthetic transactions.

There are multiple strategies that can be employed to deliver SOX and performance information. Dashboards (Figure 3) are the preferred approach for real-time Control Point breach notifications. Reports are the preferred delivery method for weekly, monthly, quarterly, and/or annual analysis.



This provides a quick overview of our current financial situation. For more information, contact John.

© 2003, Managed Objects · All rights reserved

Figure 3. Process owner dashboard showing Control Point monitoring

Tailoring information for the recipient is highly recommended and desirable.

A lot of information will be captured as part of Control Point monitoring. Process owners should be notified and afforded the opportunity to research and resolve the Control Point breach. Filtering information is therefore essential so that recipients are notified only of ongoing issues. Incorporating filtering safeguards prevents rushed problem notifications to higher-level managers. Threshold screening, filtering and notification deferral are important for certifying officers (i.e., the executive team). They are only interested in knowing critical breaches or issues, not all incidents.

Creating an operational data store (ODS) is essential to provide long-term storage of the information (evidence). Content Management software can be utilized to enforce storage rules and to maintain your information. BAM/BSM, Content Management, Business Intelligence as well as collaboration software can be used to build, store, and deliver information through reports and dashboards.

Use of Collaboration Software for Verification, Validation, and Certification of Control Points

The steps to perform verification and validation for Disclosure Controls and Internal Controls should be scheduled, documented (to provide evidence for auditors), and then certified. The recommended approach is shown in Figure 4.

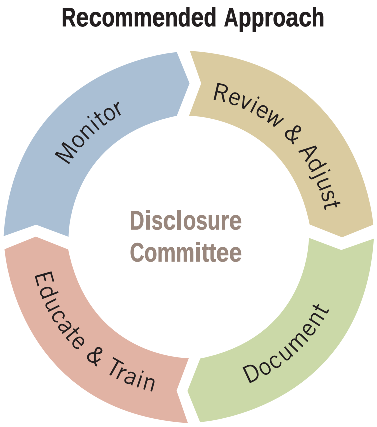


Figure 4. CEO and CFO Certifications

The Fujitsu SOX Framework outlines collaboration software that can be exploited to schedule and advance documents/approvals among all stakeholders.

In many cases, the CEO will look to his direct reports to certify their respective results. Those reports will look their management team to do the same—and so on. Collaboration software can manage the entire process and maintain an audit trail in case “evidence” is necessary at a future time.

Summary

The Sarbanes-Oxley Act has established a new approach for corporate responsibility, accountability, transparency, and behavior. The Act has ushered in a new standard for companies regarding the reporting of Control Point effectiveness.

We recommend that enterprises employ the Fujitsu SOX Framework or a similar approach to meet their Sarbanes-Oxley compliance obligations. Furthermore, organizations should utilize best practices for threshold screening, filtering, and notification deferral for certifying officers and executive notifications, dashboards, and reporting. Organizations should leverage the domains of software and principles identified in the Fujitsu SOX Framework to establish and automate the surveillance / monitoring of Control Points. Also, it is important to note that construction and implementation of a Control Point monitoring system requires expertise in many areas. This expertise must come not only from existing systems and applications, but the areas of Business Activity Monitoring, Content Management, Re-performance testing, Dashboard Design, Collaborative Software, and of course, Project Management. Lastly, you should follow COSO principles in your SOX implementation.

Good Control Point management is not just a best practice. The Act requires it through law.

About Fujitsu Consulting

A trusted provider of management and technology consulting to business and government, Fujitsu Consulting is the North American consulting and services arm of the $43.2-billion Fujitsu group. Fujitsu Consulting integrates the core expertise of the Fujitsu companies and its partners to deliver complete solutions in the areas of enterprise information management, packaged application implementation, legacy systems modernization, IT governance, managed services and business process services. Through its full range of IT consulting, implementation and management services and its industry-recognized strategic approach, Macroscope®, Fujitsu Consulting enables clients to build more value into their IT investments and drive their leadership in the marketplace.

We work with you to create solutions and produce results that drive your business.

Headquarters & United States
343 Thornall Street
Suite 630
Edison, NJ 08837
United States
Tel: +1 732 549 4100
Fax: +1 732 549 2375

Canada
155 University Avenue
Suite 1600
Toronto, Ontario
Canada M5H 3B7
Tel: +1 416 363 8661
Fax: +1 416 363 4739

Quebec
1000 Sherbrooke Street West
Suite 1400
Montreal, Quebec
Canada H3A 3R2
Tel: +1 514 877 3301
Fax: +1 514 877 3351

India
A-15, MIDC Technology Park
Talwade, Pune – 412 114
Maharashtra, India
Tel: +91 20 2769 0001
Fax: +91 20 2769 2924

Powered by MACROSCOPE

www.fujitsu.com